International Journal of Research in Engineering, Science and Management
Volume 6, Issue 6, June 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

A Survey on Cyber Security Threats and its Impact on Society

T. Amalraj Victoire[1], M. Vasuki[2], A. Karunamurthy[3], D. Soundarya[4*], S. Sarumathi[5]
[1,2,3]*Associate Professor, Department of MCA, Sri Manakula Vinayagar Engineering College, Puducherry, India*
[4,5]*Student, Department of MCA, Sri Manakula Vinayagar Engineering College, Puducherry, India*

***Abstract*: Cyber security is essential to society as protecting information, computer networks, databases, and software programs has become one of the biggest challenges in the current day situation. The Internet plays a vital role in day-to-day people's life and users expect their data to be much more secure. Cyber Security threats are clarified to make the data secure. The Cyber Security threats affect society in many ways by stealing our personal information in our everyday lives and overcome those threats by securing the data from the internet. This paper concentrates on the survey of different threats to analyze and improve data security and enhance confidentiality.**

***Keywords*: Cyber security, data security, confidentiality threats, internet, personal information, survey, improve enhance.**

1. Introduction

Cyber security is the exercise of shielding computers, servers, cell devices, digital systems, networks, and data from malicious attacks.

As cyberattacks turn out to be greater and more sophisticated and corporate networks develop greater complex, lots of cyber protection solutions are required to mitigate company cyber risk. A cybersecurity threat is a malicious act supposed to steal or borrow or harm information or damage or disrupt the virtual well-being and balance of an enterprise. Cyber threats encompass a massive range of attacks ranging from data breaches, to computer viruses, denial of service, and numerous exclusive attack vectors.

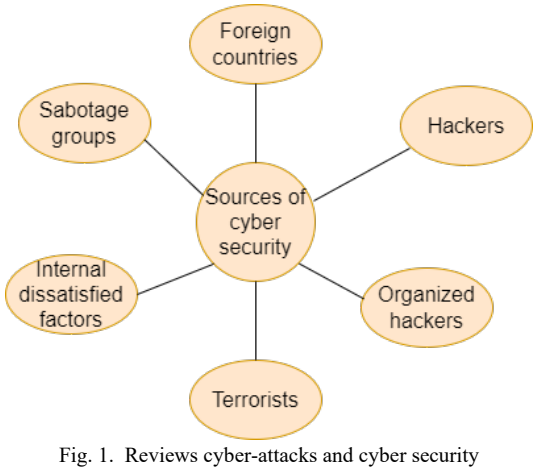

Fig. 1. Reviews cyber-attacks and cyber security

It is also referred to as a potential cyberattack that aims to gain unauthorized access, disrupt, steal, or harm an IT asset, intellectual property, computer network, or any other form of sensitive data. Threats can come from relied customers from within an enterprise and remote locations with the aid of using unknown external parties. There are different types of cyber threats that are classified into different types.

2. Literature Survey

Harri Ruoslathi and Brid Davis (2021). Societal Impacts of Cyber Security Assets of Project ECHO. This paper discusses the societal impacts of cyber security assets, such as the Project ECHO project, which aims to improve the resilience of critical infrastructure to cyber-attacks. The paper argues that cyber security assets can have a positive impact on society by reducing the risk of cyber-attacks, improving the availability of critical services, and protecting personal data. Abel Yeboah-Ofori, Shareeful Islam, Sin Wee Lee, et al. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. This paper proposes a cyber threat predictive analytics framework for improving cyber supply chain security. The framework uses machine learning to identify and predict cyber threats, and to recommend mitigation strategies. The paper argues that the framework can help to reduce the risk of cyber-attacks on cyber supply chains. Qi Li, Weishi Li, Junfeng Wang, et al. (2019). A SQL Injection Detection Method Based on Adaptive Deep Forest. This paper proposes a new method for detecting SQL injection attacks. The method uses an adaptive deep forest model to identify malicious SQL queries. The paper argues that the method is more effective than traditional methods for detecting SQL injection attacks. Yaoqi Yang, Xianglin Wei, Renhui Xu, et al. (2020). Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency. This paper proposes a new method for detecting and localizing man-in-the-middle attacks. The method uses cross-layer location consistency to identify malicious traffic. The paper argues that the method is more effective than traditional methods for detecting and localizing man-in-the-middle attacks. Alireza Esfahani, Georgios Mantas, Jose Ribeiro, et al. (2019). An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in

*Corresponding author: dsoundarya1512@gmail.com

Industry 4.0 Supply Chain. This paper proposes a new web authentication mechanism that can prevent man-in-the-middle attacks in Industry 4.0 supply chains. The mechanism uses a combination of public key cryptography and digital signatures to authenticate users and protect the confidentiality of communications. Keren L.G. Snider, Ryan Shandler, Shay Zandani, and Daphna Canetti (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. This paper examines the relationship between cyberattacks, cyber threats, and attitudes toward cybersecurity policies. The paper argues that people's attitudes toward cybersecurity policies are influenced by their experiences with cyberattacks and cyber threats. Sultan Asiri, Yang Xiao, Saleh Alzahrani, et al. (2023). A Survey of Intelligent Detection Designs of HTML URL Phishing Attacks. This paper surveys the literature on intelligent detection designs of HTML URL phishing attacks. The paper discusses the different types of HTML URL phishing attacks, and the different methods that have been proposed for detecting them. Innocent Mbona and Jan H.P. Eloff (2022). Classifying social media bots as malicious or benign using semi-supervised machine learning. This paper proposes a semi-supervised machine learning method for classifying social media bots as malicious or benign. The method uses a combination of supervised and unsupervised learning techniques to classify social media bots. Md.Sakir Hossain, Naim Hasan, Md.Abdus Samad, et al. (2022). Android Ransomware Detection from Traffic Analysis Using Metaheuristic Feature Selection. This paper proposes a new method for detecting Android ransomware from traffic analysis. The method uses metaheuristic feature selection to identify the most important features for detecting ransomware.

1) Malware

Malware is malicious software programs together with spyware, ransomware, contagions, and worms. Malware is actuated when a person clicks on a vicious hyperlink or attachment, which ends up in installing dangerous software.

2) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

The purpose of the Denial-of-Service assault is to make the service unavailable by flooding or crashing the system with voluminous traffic that the server can't accommodate.

In DoS, a single hacker/attacker penetrates the victim's system; whereas, in DDoS, more than one attacker penetrates the victim's system.

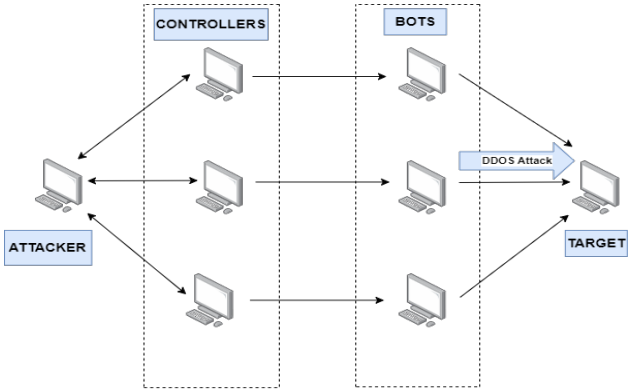

Fig. 2. Denial-of-Service (DDoS) attacks

3) 3. Drive-by Attack

When the system has security flaws due to a lack of updates on the OS, app, or browser, an attacker can cause the unintended download of malicious code to the targeted pc or cellular device, making it vulnerable.

In this attack, the victim does not necessarily click on any links, open a malicious e-mail attachment, or download any files.

Table 1

	Impact on Society	Overcoming methods
1.	In Financial Losses, malware can cause substantial financial losses to individuals and businesses and in data breaches it is mainly used to steal sensitive information, such as personal data, financial records, or intellectual property.	The malware threats can be overcome by the following: By Implementing Robust security measures in various fields like installing reputable antivirus software and keep it up to date, utilizing firewalls and intrusion detection/prevention systems to protect networks and by using encryption for sensitive data for both at rest and during transmission.
2.	The Disruption of Critical Infrastructure uses these threats to target critical infrastructure systems, such as power grids, transportation networks, or healthcare facilities. False information, propaganda, or fake news can be spread through malware threats, which implemented the Spread of Propaganda and Fake News.	Practice Safe Internet and Email Usage enables by exercising caution when clicking on links or downloading attachments from unfamiliar or suspicious sources, being aware of phishing attempts, and avoiding providing sensitive information via email or untrusted websites. It also enables regular using antivirus software to scan email attachments and downloaded files for malware.
3.	Global Cybersecurity Challenges involve malware threats which are a global concern, transcending borders and impacting societies worldwide. They highlight the need for international collaboration to combat cybercrime effectively. Malware attacks, which cross national boundaries and have an effect on civilizations all over the world, are one of the global cybersecurity challenges. They emphasise the necessity of international cooperation in the successful eradication of cybercrime. In order to exchange threat intelligence, create effective security measures, and create legal frameworks for prosecuting cybercriminals, governments, organisations, and people must collaborate.	Educate Users on Cybersecurity Best Practices used to conduct regular training sessions to educate individuals about safe browsing habits, recognizing phishing attempts, and avoiding suspicious downloads or websites and it promotes the use of strong, unique passwords and enables two-factor authentication (2FA) wherever possible, it also encourages the users to report any suspected security incidents or unusual system behaviours promptly. To stay up to date on new threats and mitigation techniques, foster collaboration and information sharing with trusted partners, industry groups, and cybersecurity organizations. Additionally, work with law enforcement organizations to report cybercrime incidents and support investigations.
4.	Productivity and Operational Losses using malware infections can lead to significant productivity losses for individuals and organizations. Infected systems may experience performance degradation, crashes, or unavailability, impacting day-to-day operations. Moreover, organizations may need to invest time and resources in malware removal, system restoration, and strengthening security measures, diverting attention from core activities.	To stay up to date on new threats and mitigation techniques, foster collaboration and information sharing with trusted partners, industry groups, and cybersecurity organizations. Additionally, work with law enforcement organizations to report cybercrime incidents and support investigations.

Table 2

	Impact on Society	Overcoming methods
1.	Opportunity for Cybercrime using DDoS attacks can serve as a diversionary tactic for cybercriminals. While the targeted organization is dealing with the attack, criminals may exploit the chaos to carry out other malicious activities, such as data breaches, theft, or sabotage.	The attacks Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) can be overcome by the following: Access Control Lists (ACLs) use access control lists to restrict access to your network and services. By only allowing trusted IP addresses or specific user groups to access your systems, you can minimize the risk of unauthorized access and potential attacks.
2.	Political and Activism Motives using DDoS attacks have been used as a means of protest or activism by groups or individuals seeking to voice their grievances. While their intentions may vary, such attacks can disrupt government websites, financial institutions, or critical infrastructure, impacting public services and causing public inconvenience or concern.	Collaborating with ISPs and DDoS Mitigation Services involves establishing relationships with your Internet Service Provider (ISP) and considering engaging with specialized DDoS mitigation services. These entities can help detect and block malicious traffic before it reaches your network, minimizing the impact of an attack.
3.	Infrastructure Vulnerabilities using these DDoS attacks can expose vulnerabilities in network infrastructures and systems. Organizations are forced to assess their security measures and enhance their defences against future attacks. This ongoing battle between attackers and defenders drives advancements in cybersecurity and network resilience.	Traffic Scrubbing and Filtering are used to employ traffic scrubbing services that can detect and filter out malicious traffic, diverting only legitimate traffic to your network. These services can help identify and drop DDoS attack traffic while allowing genuine users to access your services.

Table 3

	Impact on Society	Overcoming methods
1.	Malware Infections often result in the installation of malware on victims' devices. This malware can perform various malicious activities, including stealing sensitive information, damaging or encrypting files, or turning devices into botnets for launching further attacks. The impact includes financial losses, loss of data, and compromised privacy.	The Drive-by Attacks can be overcome by the following: Utilize browser security features uses Web browsers often have built-in security features that can help protect against drive-by attacks. Enable pop-up blockers, anti-phishing filters, and warnings for potentially malicious websites.
2.	Privacy Violations can utilize drive-by attacks that exploit vulnerabilities in web browsers or plugins can result in privacy violations. Attackers can track users' online activities, capture sensitive information, or spy on individuals through unauthorized access to their devices. This intrusion on privacy can lead to personal and psychological harm.	While downloading or running possibly suspicious files, visualize using a sandbox or virtual environment. This isolates the activity from your main system, reducing the risk of infection. Implement a web filtering system to stop users from unintentionally visiting known harmful websites by blocking access to them.
3.	Drive-by assaults can be employed as a component of larger social engineering strategies, such as social engineering exploitation. By sending misleading emails or texts, attackers can deceive users into accessing compromised sites or clicking on harmful links. This may result in identity theft, user behaviour manipulation, or the dissemination of false information.	Use an ad-blocker to prevent drive-by attacks, which can occasionally be caused by advertisements on websites. Installing an ad-blocker can help reduce the risk of encountering malicious ads. Employing network security measures can implement firewalls, intrusion detection and prevention systems, and secure network configurations to help safeguard your network from external threats.

Table 4

	Impact on Society	Overcoming methods
1.	Phishing attacks using identity theft can be a precursor to identity theft and by tricking users into revealing personal information, attackers can assume their identities, potentially leading to fraudulent activities, unauthorized account access, and damage to the victims' reputations.	The phishing threats can be overcome by the following: To avoid clicking on suspicious links or attachments refrain from clicking on links or opening attachments from unknown or suspicious sources and these can lead to malicious websites or initiate malware downloads.
2.	Phishing attacks utilize time and productivity loss can consume significant time and resources for individuals and organizations, it deals with the aftermath of an attack, such as recovering compromised accounts, reporting incidents, and implementing more robust security measures, which can be time-consuming and disruptive.	Never share personal or financial information as legitimate organizations will never ask for sensitive information such as passwords, social security numbers, or credit card details via email or unsolicited phone calls. Be cautious and avoid providing such information unless you have verified the authenticity of the request through a trusted channel.
3.	Reputational damage uses organizations that fall victim to phishing attacks can suffer reputational damage and once the customer trust is compromised, it can be challenging to regain, potentially resulting in a loss of business and credibility.	By using strong and unique passwords which maintain strong, unique passwords for all your online accounts, avoid using common passwords or reusing passwords across multiple accounts, and consider using a password manager to securely store and generate complex passwords.

4) Phishing

Phishing attacks use fake communication, inclusive of an email, to trick the receiver into opening it and carrying out the instructions inside, which include presenting a credit card number. The aim is to steal sensitive records like credit card and login information or to install malware on the victim's machine.

5) Password Attack

With the proper password, a cyber attacker has to get entry to a wealth of information. Social engineering is a kind of password assault that Data Insider defines as "a method cyber attackers use that is predicated closely on human interaction and regularly entails tricking humans into breaking standard security practices." Other types of password assaults encompass gaining access to a password database or outright guessing.

6) Man in the Middle Attacks

A man-in-the-middle (MITM) assault takes place while hackers insert themselves into a two-party transaction.

After interrupting the traffic, they could clear out and steal the data. MITM assaults frequently arise while a visitor makes use of an unsecured public Wi-Fi network. Attackers insert themselves among the visitor and the network, after which use malware to put in software programs and use information maliciously.

Table 5

	Impact on Society	Overcoming methods
1.	Cybercrime and fraud including compromised passwords can enable cybercriminals to conduct various fraudulent activities, such as unauthorized financial transactions, phishing attacks, or ransomware incidents and these crimes can disrupt businesses, cause financial harm, and undermine confidence in online platforms and services.	The password attacks can be overcome by the following: Using complex and unique passwords can create passwords that are at least eight characters long and include a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using common words or sequential patterns.
2.	Increased cybersecurity costs involve organizations and individuals often incur substantial costs in response to password threats. This includes implementing stronger security measures, conducting forensic investigations, providing identity theft protection services, and addressing legal or regulatory obligations.	Avoid password reuse which is never reusing passwords across multiple accounts. If one account gets compromised, it could potentially give unauthorized access to your other accounts. Use a password manager to help you generate and securely store unique passwords for each account.
3.	The proliferation of password reuses when the passwords are compromised, individuals may reuse the same or similar passwords across multiple accounts. This practice increases the likelihood of further security breaches and amplifies the impact of password threats.	Monitor account activity checks regularly and reviews your account activity and statements to identify any unauthorized access or suspicious transactions. Report any suspicious activity to the respective service provider immediately.

Table 6

	Impact on Society	Overcoming methods
1.	Trust Erosion uses MITM attacks to undermine trust in communication channels and online services. When users are aware that their communications or transactions can be intercepted and manipulated, they may become hesitant to use online services, conduct e-commerce, or share sensitive information.	The Man in the Middle Attacks can be overcome by the following: Avoid public Wi-Fi networks that are particularly vulnerable to MitM attacks. Avoid connecting to untrusted or public Wi-Fi networks, especially when performing sensitive activities like online banking or accessing confidential information. If necessary, use a virtual private network (VPN) to establish an encrypted and secure connection.
2.	Businesses may experience major interruptions as a result of MITM attacks. Financial losses, reputational harm, or damaged business ties may result if an attacker successfully intercepts and alters conversations between business partners.	Two-factor authentication (2FA) which enables two-factor authentication (2FA) whenever possible. By requiring an additional verification step, such as a unique code sent to a mobile device, 2FA adds an extra layer of security and makes it more difficult for attackers to gain unauthorized access.
3.	Data Theft used by the Attackers can exploit MITM attacks to steal valuable data such as credit card information, social security numbers, and intellectual property. The affected individuals or organizations may suffer financial losses as well as personal injury as a result of utilizing the stolen data for identity theft, financial fraud, or even selling it on the black market.	Verify digital certificates are accessing the websites or online services that require authentication, always verify the validity of digital certificates. Check for secure connection indicators, such as a padlock icon or HTTPS in the URL. Be cautious if you receive any certificate warnings or errors and avoid proceeding if there are suspicions.

7) Emotet

Emotet is a sort of malware originally designed as a banking Trojan aimed toward stealing monetary data, however, it's advanced to grow to be a major threat to customers everywhere. Emotet has been regarded to deceive basic antivirus packages and hide from them. Once infected, the malware spreads like a computer virus and tries to infiltrate different computer systems with inside the network.

8) SQL Injection

A Structured Query Language (SQL) injection is a form of cyber assault that effects from placing malicious code right into a server that makes use of SQL.

Submitting the malicious code may be as easy as coming into it right into a vulnerable internet search box.

9) Ransomware

In a ransomware attack, the goal is to download ransomware from an internet site or inside an e-mail attachment.

The malware is written to make the most vulnerabilities that have no longer been addressed through the system's manufacturer or the IT team.

At times, ransomware may be used to assault more than one event with the aid of using denying access to both numerous computer systems or a central server essential to business operations.

10) DNS Spoofing

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once at the fraudulent site, the sufferer might also additionally enter sensitive information that may be used or offered with the aid of using the hacker. The hacker might also assemble a poor-quality web page with derogatory or inflammatory content material to make a competitor's enterprise look bad.

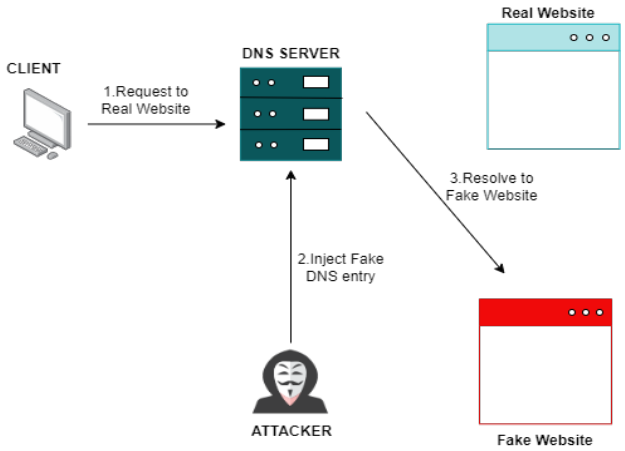

Fig. 3. DNS spoofing

11) Malware

Malware threats have significant impacts on society, affecting individuals, organizations, and even governments. Overcoming malware threats requires a proactive and multi-faceted approach combining technical measures, combines technical measures and awareness, and effective cybersecurity practices.

Table 7

	Impact on Society	Overcoming methods
1.	Global Reach and Collaboration uses the emotet to operate internationally, focusing on people, companies, and governments in a variety of countries. It highlighted the value of international cooperation and information sharing to combat such threats and illustrated the efficiency of a globally coordinated cybercriminal operation.	The Emotet Attacks can be overcome by the following: Patching and Updates are made to keep all operating systems, software, and applications up to date with the latest security patches and regularly check for updates and apply them promptly to address any known vulnerabilities.
2.	Spreading Other Malware by emotet had worm-like capabilities, allowing it to propagate and infect other systems within the same network. It acted as a delivery mechanism for other types of malwares, such as ransomware and credential stealers. This meant that an emotet infection could lead to further damage and data loss through subsequent malware attacks.	Continuous Monitoring and Threat Intelligence are used to implement robust monitoring systems to detect suspicious activities and network anomalies and stay updated on the latest threat intelligence reports and indicators of compromise related to Emotet.
3.	Spreading Other Malware by emotet had worm-like capabilities, allowing it to propagate and infect other systems within the same network. It acted as a delivery mechanism for other types of malwares, such as ransomware and credential stealers.	Strong Email Security is used to deploy a reliable email filtering solution that can detect and block malicious attachments or links. Implement strict email policies, such as blocking certain file types or using email authentication protocols like DMARC, SPF, and DKIM.

Table 8

	Impact on Society	Overcoming methods
1.	Privacy violations used by SQL injection attacks can compromise the privacy of individuals by exposing personal information or allowing unauthorized access to private databases. This can lead to an invasion of privacy, identity theft, stalking, or other forms of harassment.	The SQL injection Attacks can be overcome by the following: The Least Privilege Principle are ensuring that the database user account used by your application has the least privileges necessary to perform its intended tasks. Limit the account's permissions to only the required tables, stored procedures, and functions.
2.	Data breaches used by SQL injection attacks can lead to unauthorized access to sensitive data such as personal information, financial records, or intellectual property. Data breaches can have severe consequences for individuals, organizations, and society as a whole, including financial losses, identity theft, and reputational damage.	Escaping Special Characters that cannot be used in parameterized queries or prepared statements, make sure to escape special characters in the user input. Most programming languages provide built-in functions or libraries to escape special characters, such as adding slashes () in PHP or parameterized queries in frameworks like Hibernate for Java.
3.	System disruptions used by SQL injection attacks can disrupt the normal functioning of web applications and databases. Attackers may modify or delete data, corrupt databases, or inject malicious code that can lead to system crashes or denial-of-service conditions. These disruptions can negatively impact productivity, customer experiences, and the availability of critical services.	Implement Database Whitelisting is used to create a whitelist of allowed characters for each input field. Validate the input against these whitelists and reject any input that contains disallowed characters. This approach can help prevent attackers from injecting SQL code.

Table 9

	Impact on Society	Overcoming methods
1.	Diminished Trust is using the occurrence of ransomware attacks to erode trust in digital systems and services. When organizations cannot protect their data, customers, clients, or users may lose confidence safeguarding personal information, leading to decreased trust in online transactions and communication.	The Ransomware Attacks can be overcome by the following: Use Endpoint Protection is used to deploy endpoint protection solutions, including antivirus software, anti-malware tools, and host-based intrusion prevention systems (HIPS), on all devices. These tools can detect and block ransomware infections and other malware.
2.	Economic Impact using these ransomware attacks can have broader economic implications. If a significant number of organizations or critical infrastructure systems are targeted, the overall productivity of a region or country can be affected, leading to economic losses on a larger scale.	Employ Email and Web Filtering is used to implement robust email and web filtering solutions to block malicious attachments, links, and websites commonly used by attackers. These filters can help prevent ransomware from reaching your network in the first place.
3.	Data Loss and Leakage are used in some cases, victims of ransomware attacks may lose their data permanently if they don't have proper backups. The attackers may also threaten to release sensitive or confidential information publicly if the ransom demands are not met, potentially causing reputational damage or compromising privacy.	Incident Response Plan is used to develop an incident response plan that outlines the steps to be taken in case of a ransomware attack. This plan should include steps for isolating affected systems, reporting the incident to appropriate authorities, and communicating with affected parties.

Table 10

	Impact on Society	Overcoming methods
1.	Reduced Internet Trust in DNS spoofing attacks undermines the trust users have in the DNS infrastructure. This can lead to decreased confidence in online communication, e-commerce, and other internet-based activities, hindering societal progress and economic growth.	The DNS Spoofing Attacks can be overcome by the following: Use a reliable DNS server that ensures that you are using a trustworthy DNS server provided by your Internet Service Provider (ISP) or a reputable third-party DNS provider. Reliable DNS servers are less likely to be compromised or susceptible to spoofing.
2.	Disruption of Online Services in DNS spoofing can be used to redirect users away from legitimate websites or services, causing inconvenience and disruption. This can affect businesses, online platforms, and even critical infrastructure if DNS servers are compromised.	Monitor DNS traffic which regularly monitors your DNS traffic for any suspicious or unexpected activities. Anomalies in DNS requests or responses may indicate a DNS spoofing attack. Intrusion detection and prevention systems (IDPS) can be used to detect and mitigate such attacks.
3.	Phishing and Malware Distribution in which the Attackers can redirect users to fake websites that imitate legitimate ones, aiming to steal sensitive information such as login credentials, credit card details, or personal data. Additionally, they can manipulate DNS responses to distribute malware or exploit vulnerabilities in users' systems.	Implement the DNS Security Extensions (DNSSEC) is a set of security measures that add digital signatures to DNS data, preventing the modification or spoofing of DNS responses. DNSSEC can provide authentication and integrity to DNS records, making it harder for attackers to manipulate DNS responses.

12) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are malicious attempts to disrupt the normal functioning of a computer network, system, or service by overwhelming it with a flood of illegitimate requests or traffic. While DoS attacks originate from a single source, DDoS attacks involve multiple sources or devices, often forming a botnet, to launch the attack. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks can be challenging to mitigate, but there are several measures you can take to overcome them.

13) Drive-by Attack

Drive-by attacks pose several threats to individuals and society as a whole. These threats can have significant impacts on various aspects of society. Overcoming drive-by attack threats requires a combination of proactive measures and security best practices.

14) Phishing

The impact of phishing attacks on society can be significant and far-reaching. To mitigate the impact of phishing attacks, it is crucial for individuals and organizations to remain vigilant. Overcoming phishing threats that occur in society, it's important to adopt proactive measures and educate oneself and others about phishing attacks.

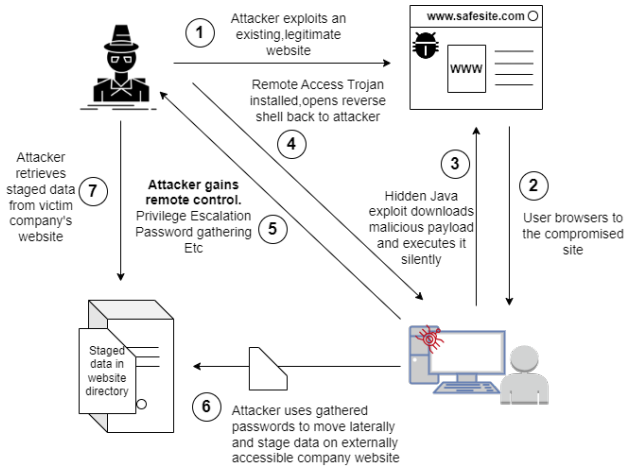

Fig. 4. Drive-by download attack

15) Password Attacks

Password threats can have significant impacts on society, both at an individual level and on a larger scale. Overcoming password threats in society requires implementing strong security practices and adopting additional measures to protect sensitive information.

16) Man in the Middle Attacks

A Man-in-the-Middle (MITM) attack is a form of cyber-attack where an attacker intercepts and potentially alters communications between two parties without their knowledge or consent. The impact of Man-in-the-Middle attacks on society can be significant and far-reaching. By implementing these measures and staying informed about the latest security best practices, individuals and organizations can significantly reduce the risk of falling victim to MitM attacks.

17) Emotet Attacks

Emotet was primarily distributed through spam emails containing malicious attachments or links, which, when clicked or opened, would infect the victim's computer. The impact of Emotet attacks on society was significant and far-reaching. Overcoming an Emotet attack requires a combination of preventive measures and effective response strategies.

18) SQL Injection Attacks

SQL injection is a type of cybersecurity attack that targets web applications by manipulating the input parameters of SQL queries. The goal is to exploit vulnerabilities in the application's database layer and gain unauthorized access to data or perform malicious actions within the system. SQL injection attacks can have significant impacts on society. To overcome SQL injection attacks, you should follow secure coding practices and implement preventive measures.

19) Ransomware Attacks

Ransomware attacks are a type of malicious cyber-attack where the attacker encrypts the victim's data and demands a ransom payment in exchange for restoring access to the data. The impact of ransomware attacks on society can be significant and far-reaching. These attacks can be devastating, but there are several steps you can take to mitigate the risks and protect yourself and your organization.

20) DNS Spoofing

DNS spoofing is a type of cyber-attack where an attacker manipulates the Domain Name System (DNS) to redirect users to fraudulent websites or intercept their communications records, attackers can redirect users to malicious websites or intercept their traffic, leading to various negative consequences. The impact of DNS spoofing attacks on society can be significant and wide-ranging. To overcome DNS spoofing attacks and enhance security, these are the following measures.

3. Conclusion

cyber security threats are a serious issue that affects society in many ways. The internet has become an essential part of our lives, and we rely on it for everything from communication to banking. As a result, our personal and financial information is increasingly vulnerable to cyber-attacks. There are a number of different types of cyber security threats, including malware, phishing, and social engineering. These threats can have a significant impact on individuals and organizations, both financially and reputationally. In order to protect ourselves from cyber security threats, it is important to be aware of the risks and to take steps to mitigate them. Some of the things we can do include using strong passwords, keeping software up to date, and being aware of phishing scams. We must also work to educate ourselves and others about cyber security threats. The more we know about these threats, the better we can protect ourselves from them.

References

[1] Harri Ruoslathi, Brid Davis, “Societal Impacts of Cyber Security Assets of Project ECHO,” Volume 17, December 2021.

[2] Abel Yeboah-Ofori, Shareeful Islam, Sin Wee Lee, Zia Ush Shamszaman, Khan Muhammad, Meteb Altaf, Mabrook S.Al-Rakhami, “Cyber Threat

Predictive Analytics for Improving Cyber Supply Chain Security," in Volume 9, June 2021.

[3] Qi Li, Weishi Li, Junfeng Wang, Mingyu Cheng, "A SQL Injection Detection Method Based on Adaptive Deep Forest," Volume 7, October 2019.

[4] Yaoqi Yang, Xianglin Wei Renhui Xu, Laixian Peng, Lei Zhang, Lin Ge, "Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency," Volume 8, June 2020.

[5] Alireza Esfahani, Georgios Mantas, Jose Ribeiro, Joaquim Bastos, Shahid Mumtaz, Manuel A. Violas, A. Manuel De Oliveira Duarte, Jonathan Rodriguez, "An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4.0 Supply Chain," Volume 7, April 2019.

[6] Keren L.G. Snider, Ryan Shandler, Shay Zandani and Daphna Canetti, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," August 2021.

[7] Sultan Asiri, Yang Xiao, Saleh Alzahrani, Shuhui Li, Tieshan Li, "A Survey of Intelligent Detection Designs of HTML URL Phishing Attacks," Volume 11, January 2023.

[8] Innocent Mbona, Jan H. P. Eloff, "Classifying social media bots as malicious or benign using semi-supervised machine learning," October 2022.

[9] Md. Sakir Hossain, Naim Hasan, Md. Abdus Samad, Hossain Md. Shakhawat, Joydeep Karmoker, K. F. M. Nafiz Fuad, Kwonhue Choi, "Android Ransomware Detection from Traffic Analysis Using Metaheuristic Feature Selection," Volume 10, December 2022.

[10] Keren L.G. Snider, Ryan Shandler, Shay Zandani and Daphna Canetti, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," August 2021.

[11] Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

[12] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1), 69-104.

[13] Herley, C. (2009). So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. Proceedings of the 2009 Workshop on New Security Paradigms, 133-144.

[14] Lipinski, M., & Lipinski, P. (2015). Social Engineering in the Cyberspace: Psychological Perspective of Manipulation Techniques Used in Cyber Crimes. Journal of Applied Security Research, 10(3), 373-395.

[15] McQueen, R. J., & Mahmoud, Q. H. (2009). Cyber Security and Information Assurance Challenges in Smart Grids. Proceedings of the 42nd Hawaii International Conference on System Sciences, 1-10.